§ 501.13 False representations of Postal Service actions.

Providers, their agents, and employees must not intentionally misrepresent to customers of the Postal Service decisions, actions, or proposed actions of the Postal Service respecting its regulation of Postage Evidencing Systems. The Postal Service reserves the right to suspend and/or revoke the authorization to manufacture or distribute Postage Evidencing Systems throughout the United States or any part thereof pursuant to § 501.6 when it determines that the provider, its agents, or employees failed to comply with this section.

§ 501.14 Postage Evidencing System inventory control processes.

(a) Each authorized provider of Postage Evidencing Systems must permanently hold title to all Postage Evidencing Systems which it manufactures or distributes except those purchased by the Postal Service or distributed outside the United States.

(b) An authorized provider must maintain sufficient facilities for and records of the distribution, control, storage, maintenance, repair, replacement, and destruction or disposal of all Postage Evidencing Systems and their components to enable accurate accounting and location thereof throughout the entire life cycle of each Postage Evidencing System. A complete record shall entail a list by serial number of all Postage Evidencing Systems manufactured or distributed showing all movements of each system from the time that it is produced until it is scrapped, and the reading of the ascending register each time the system is checked into or out of service. These records must be available for inspection by Postal Service officials at any time during business hours.

(c) To ensure adequate control over Postage Evidencing Systems, plans for the following processes must be submitted for prior approval, in writing, to PTM:

(1) Check in to service procedures for all Postage Evidencing Systems—the procedures are to address the process to be used for new Postage Evidencing Systems as well as those previously leased to another customer.

(2) Transportation and storage of meters—procedures that provide reasonable precautions to prevent use by unauthorized individuals. Providers must ship all meters by Postal Service Registered Mail unless given written permission by the Postal Service to use another carrier. The provider must demonstrate that the alternative delivery carrier employs security procedures equivalent to those for Registered Mail.

(3) Postage meter examination/inspection procedures and schedule—The provider is required to perform postage meter examinations or inspections based on an approved schedule. Failure to complete the meter examination or inspections by the due date may result in the Postal Service requiring the provider to disable the meter's resetting capability. If necessary, the Postal Service shall notify the customer that the meter is to be removed from service and the authorization to use a meter revoked, following the procedures for revocation specified by regulation. The Postal Service shall notify the provider to remove the meter from the customer's location.

(4) Check out of service procedures for a non-faulty Postage Evidencing System when the system is to be removed from service for any reason.

(5) Postage meter repair process—any physical or electronic access to the internal components of a postage meter, as well as any access to software or security parameters, must be conducted within an approved facility under the provider's direct control and active supervision. To prevent unauthorized use, the provider or any third party acting on its behalf must keep secure any equipment or other component that can be used to open or access the internal, electronic, or secure components of a meter.

(6) Faulty meter handling procedures, including those that are inoperable, mis-registering, have unreadable registers, inaccurately reflect their current status, show any evidence of possible tampering or abuse, and those for which there is any indication that the meter has some mechanical or electrical malfunction of any critical security component, such as any component the improper operation of which

could adversely affect Postal Service revenues, or of any memory component, or that affects the accuracy of the registers or the accuracy of the value printed.

(7) Lost or stolen meter procedures—the provider must promptly report to the Postal Service the loss or theft of any meter or the recovery of any lost or stolen meter. Such notification to the Postal Service will be made by completing and filing a standardized lost and stolen meter incident report within ten (10) calendar days of the provider's determination of a meter loss, theft, or recovery.

(8) Postage meter destruction, when required-the postage meter must be rendered completely inoperable by the destruction process and associated postage—printing dies and components must be destroyed. Manufacturers/distributors of meters must submit the proposed destruction method; a schedule listing the postage meters to be destroyed, by serial number and model; and the proposed time and place of destruction to PTM for approval prior to any meter destruction. Providers must record and retain the serial numbers of the meters to be destroyed and provide a list of such serial numbers in electronic form in accordance with Postal Service requirements for meter accounting and tracking systems. Providers must give sufficient advance notice of the destruction to allow PTM to schedule observation by its designated representative who shall verify that the destruction is performed in accordance with a Postal Service—approved method or process. To the extent that the Postal Service elects not to observe a particular destruction, the provider must submit a certification of destruction, including the serial number(s) to the Postal Service within five (5) calendar days of destruction. These requirements for meter destruction apply to all postage meters, Postage Evidencing Systems, and postal security devices included as a component of a Postage Evidencing System.

(d) If the provider uses a third party to perform functions that may affect Postage Evidencing System security, including, but not limited to repair, maintenance, and disposal of Postage Evidencing Systems, PTM must be advised in advance of all aspects of the relationship, as they relate to the custody and control of Postage Evidencing Systems, and must specifically authorize in writing the proposed arrangement between the parties.

(1) Postal Service authorization of a third party relationship to perform specific functions applies only to the functions stated in the written authorization but may be amended to embrace additional functions.

(2) No third-party relationship shall compromise the security of the Postage Evidencing System, or its components, including, but not limited to, the hardware, software, communications, and security components, or of any security-related system with which it interfaces, including, but not limited to, the resetting system, reporting systems, and Postal Service support systems. The functions of the third party with respect to a Postage Evidencing System, its components, and the systems with which it interfaces are subject to the same scrutiny as the equivalent functions of the provider.

(3) Any authorized third party must keep adequate facilities for and records of Postage Evidencing Systems and their components in accordance with paragraph (b) of this section. All such facilities and records are subject to inspection by Postal Service representatives, insofar as they are used to distribute, control, store, maintain, repair, replace, destroy, or dispose of Postage Evidencing Systems.

(4) The provider must ensure that any party acting on its behalf in any of the functions described in paragraph (b) of this section maintains adequate facilities, records, and procedures for the security of the Postage Evidencing Systems. Deficiencies in the operations of a third party relating to the custody and control of Postage Evidencing Systems, unless corrected in a timely manner, can place at risk a provider's approval to manufacture and/or distribute Postage Evidencing Systems.

(5) The Postal Service reserves the right to review all aspects of any third party relationship if it appears that the relationship poses a threat to Postage Evidencing System security and

may require the provider to take appropriate corrective action.

§ 501.15 Computerized Meter Resetting System.

(a) *Description.* The Computerized Meter Resetting System (CMRS) permits customers to reset their postage meters at their places of business. Authorized providers, who operate CMRS services, are known as resetting companies (RCs).

(b) A customer is required to have funds available on deposit with the Postal Service before resetting a Postage Evidencing System or the provider may opt to provide a funds advance in accordance with paragraph (c) of this section.

(c) If the RC chooses to offer advancement of funds to customers, the RC is required to maintain a deposit with the Postal Service equal to at least one (1) day's average funds advanced. The total amount of funds advanced to customers on any given day shall not exceed the amount the provider has on deposit with the Postal Service. The Postal Service shall not be liable for any payment made by the RC on behalf of a customer that is not reimbursed by the customer, since the RC is solely responsible for the collection of advances made by the RC.

(d) The CMRS customer is permitted to make deposits in one of three ways: check, electronic funds transfer (or wire transfer), or automated clearinghouse (ACH) transfer. These deposits must be remitted to the Postal Service's designated bank account.

(e) The RC must require each CMRS customer that requests a meter resetting to provide the meter serial number, the CMRS account number, and the meter's ascending and descending register readings. The RC must verify that there are sufficient funds in the customer's CMRS account to cover the postage setting requested before proceeding with the setting transaction (unless the RC opts to provide the customer a funds advance).

(f) The Postal Service requires that the RC publicize to all CMRS customers the following payment options (listed in order of preference):

(1) Automated clearinghouse (ACH) debits/credits.

(2) Electronic funds transfers (wire transfers).

(3) Checks.

(g) Returned checks and ACH debits are the responsibility of the Postal Service. Upon notice from the Postal Service's designated bank, the provider will be required to immediately lock the customer account to prevent a meter reset until the Postal Service receives payment for the returned check or the provider is provided with valid ACH credit or wire information.

(h) *Refunds.* The Postal Service will issue a refund in the amount remaining in a customer's Computerized Meter Resetting System account, after such time as the customer provides a written request to the provider, as long as the request meets the Postal Service approved minimum and time frame.

(i) *Security and Revenue Protection.* To receive Postal Service approval to continue to operate systems in the CMRS environment, the RC must submit to a periodic examination of its CMRS system and any other applications and technology infrastructure that may have a material impact on Postal Service revenues, as determined by the Postal Service. The examination shall be performed by a qualified, independent audit firm and shall be conducted in accordance with the Statement on Auditing Standards (SAS) No. 70, Service Organizations, developed by the American Institute of Certified Public Accountants (AICPA), as amended or superseded. The examination shall include testing of the operating effectiveness of relevant RC internal controls (Type II SAS70 Report). If the service organization uses another service organization (sub-service provider), Postal Service Management should consider the nature and materiality of the transactions processed by the sub-service organization and the contribution of the sub-service organization's processes and controls in the achievement of the Postal Service's information processing objectives. The Postal Service should have access to the sub-service organization's SAS 70 report. The control objectives to be covered by the SAS 70 report are subject to Postal Service review and approval and are to be provided to the